DRAFT HANDBOOK 150-20

National Voluntary Laboratory Accreditation Program

SPECIAL NOTICE – JULY 27, 1999:

DRAFT
Subject to change. Contact NVLAP Jeffrey Horlick (301) 975-4020 jeffrey.horlick@nist.gov for complete laboratory accreditation application package. Handbook 150-20 contains some but not all of the requirements for laboratory accreditation.

Information Technology Security Testing - Common Criteria

April 1999
Version 1.1

U.S. Department of Commerce
William M. Daley, Secretary

Technology Administration
Gary R. Bachula, Acting Under Secretary for Technology

National Institute of Standards and Technology
Raymond G. Kammer, Director

PREFACE

NVLAP is seeking to establish a new Laboratory Accreditation Program (LAP) for Information Technology (IT) Security Testing to meet the needs of government and the private sector for accredited laboratories to conduct IT security testing. NIST Handbook 150-20 presents the technical requirements for IT security evaluation in accordance with the *Common Criteria for Information Technology Security Evaluation* and the *Common Methodology for Information Technology Security Evaluation*. It is intended for information and use by staff of accredited laboratories, those laboratories seeking accreditation, other laboratory accreditation systems, users of laboratory services, and organizations needing information on the requirements for accreditation for Common Criteria Testing (CCT).

This handbook supplements NIST Handbook 150, *NVLAP Procedures and General Requirements*, which contains Part 285 of Title 15 of the U.S. Code of Federal Regulations (CFR) plus all general NVLAP procedures, criteria, and policies. The criteria in NIST Handbook 150 encompass the requirements of ISO/IEC Guide 25 and the relevant requirements of ISO 9002 (ANSI/ASQC Q92-1987). Handbook 150-20 contains information that is specific to CCT and interprets the Procedures and General Requirements where appropriate. It will be updated, as required, to reflect program changes.

The numbering of the sections of this handbook is patterned after Handbook 150; for example, Section 285.3 of Handbook 150 presents the description and goal of NVLAP, whereas Section 285.3 of Handbook 150-20 presents only the description of CCT. Where there is no CCT-specific information, the section number is omitted.

Questions or comments concerning this handbook should be submitted to: NVLAP, National Institute of Standards and Technology, 100 Bureau Drive, Stop 2140, Gaithersburg, MD 20899-2140; phone (301) 975-4016; fax (301) 926-2884; e-mail nvlap@nist.gov.

ACKNOWLEDGMENTS

The technical requirements and checklist for CCT laboratory accreditation were developed by Julie Connolly, of the MITRE Corporation, Robin Medlock, of Mitretek Systems, and Christine Cheetham and Charles Menk, of the National Security Agency, under the guidance of Jeffrey Horlick (NVLAP) and Keith Brewster (NSA). The authors would like to acknowledge the valuable insights and comments provided by Ellen Flahavin, Arnold Johnson, Lisa Carnahan, and Annabelle Lee (NIST). The requirements in this handbook also have been strongly influenced by the NVLAP Cryptographic Module Testing and the POSIX Laboratory Accreditation Programs.

The NVLAP Program Handbook series, begun in 1982, comprises the combined efforts of the entire NVLAP staff, both past and present.

TABLE OF CONTENTS

SUMMARY

The National Information Assurance Partnership (NIAP), a partnership between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA), is establishing a program to evaluate conformance of Information Technology (IT) products to international standards. The program is known as the NIAP Common Criteria Evaluation and Validation Scheme for Information Technology Security, abbreviated as the *Common Criteria Scheme*. The Common Criteria Scheme is establishing a NIAP Validation Body, which issues a Common Criteria Certificate for an IT security evaluation. This certificate is issued if the security evaluation has been conducted in accordance with the Scheme requirements using the *Common Criteria for Information Technology Security Evaluation* (Common Criteria) and the *Common Methodology for Information Technology Security Evaluation* (Common Methodology)[1].

NIAP has requested that NVLAP establish a program to accredit laboratories conducting security evaluations using the *Common Criteria* and *Common Methodology*. An organization desiring accreditation for Common Criteria Testing (CCT) must meet the requirements presented in this handbook and NIST Handbook 150, *NVLAP Procedures and General Requirements*. Technical requirements are explained to indicate how the NVLAP criteria are applied. NIAP, through the NIAP Validation Body, manages the day-to-day operations of the Common Criteria Scheme, while NVLAP addresses only laboratory accreditation.

Any organization (including commercial entity, manufacturer, university, or federal, state, or local government laboratory) that conducts any of the test methods that comprise CCT may apply for NVLAP accreditation. Accreditation will be granted to laboratories that comply with the conditions for accreditation as defined in NIST Handbook 150 and this handbook. Accreditation does not imply a guarantee of laboratory performance or of product test data; it is a finding of laboratory competence and conformance with the requirements for accreditation.

Testing services covered: Common Criteria-based security evaluations of Protection Profiles, Security Targets, and IT products. Appendix D contains the test method selection list, which consists of the Common Criteria APE, ASE, and EAL levels 1 through 4 assurance classes, and the corresponding *Common Methodology*. An IT product can be a single product or multiple IT products configured as an IT system or system solution to meet certain consumer needs. In either case, the testing occurs in a testing facility or a client's site (under laboratory conditions) and not in the actual operational environments. At some future time, testing services may be extended to include testing in the operational environment, but are not included at this time.

Period of accreditation: One year, renewable annually.

On-site assessment: Visit by technical experts to determine compliance with the NVLAP criteria before initial accreditation and every two years thereafter. Additional monitoring visits may occur on an as-needed basis.

Assessors: Technical experts with IT security evaluation and/or quality systems expertise who review laboratory qualifications and conduct on-site assessments.

Proficiency testing: Demonstration by a laboratory that it can conduct IT security evaluations using the *Common Criteria* and the *Common Methodology*. Proficiency testing is required for initial accreditation

[1] For more information on the Common Criteria Scheme, refer to the *Common Criteria Evaluation and Validation Scheme for Information Technology Security Technology Security Organization, Management, and Concept of Operation* (*Scheme Publication* #1). For more information on the NIAP, refer to the web site at http://niap.nist.gov.

and is conducted periodically thereafter. Advance notice and instructions are given before testing is scheduled.

Granting accreditation: Based upon compliance with criteria, proficiency testing, satisfactory on-site assessment, and resolution of deficiencies.

Fees: Payments are required as listed on the fee schedule, including fees for annual administrative/technical support, on-site assessment, and proficiency testing.

Sec. 285.1 Purpose.

NIST Handbook 150-20 presents the procedures and technical requirements of the National Voluntary Laboratory Accreditation Program (NVLAP) for laboratories seeking accreditation for conducting Information Technology (IT) security evaluations under the Common Criteria Scheme. It complements and supplements the NVLAP programmatic procedures and general requirements found in NIST Handbook 150.

The interpretive comments and additional requirements contained in this handbook tailor the general NVLAP criteria and make them specifically applicable to Common Criteria Testing (CCT). Specific circumstances under which departures from the NVLAP general procedures are allowable within the scope of CCT are also addressed in this handbook.

Sec. 285.2 Organization of procedures

(a) The numbering of the sections of this handbook is patterned after Handbook 150, *NVLAP Procedures and General Requirements*, to allow easy cross-reference.

(b) The procedures and general requirements of Handbook 150 and the interpretations and specific requirements in this handbook must be combined to produce the criteria for accreditation in CCT.

(c) In addition, the handbook contains four appendices that supplement the text:

(1) Appendix A provides examples of a Scope of Accreditation and a Certificate of Accreditation for CCT;

(2) Appendix B provides the General Operations Checklist, which NVLAP assessors use during an on-site technical assessment to evaluate a laboratory's ability to conduct testing in general;

(3) Appendix C provides the CCT Specific Operations Checklist, which NVLAP assessors use during an on-site technical assessment of a laboratory; and

(4) Appendix D lists the test methods for CCT.

Sec. 285.3 Description of the CCT program

The purpose of the CCT program is to accredit laboratories that conduct IT security evaluations using the *Common Criteria* and *Common Methodology*, ensuring that such laboratories are capable and competent to meet the needs of the Common Criteria Scheme. IT security evaluations assess a Protection Profile's, Security Target's, or IT product's conformance with a specified set of *Common Criteria* requirements.

The *Common Criteria* is a set of functional and assurance IT security requirements that were developed to provide a common baseline against which IT products and systems could be evaluated. The *Common Methodology* describes a common approach for conducting IT security evaluations using the *Common Criteria*. The *Common Criteria* and *Common Methodology* were developed and sponsored by the governments of the United States (represented by NIST and NSA), Canada, France, Germany, the Netherlands, and the United Kingdom. The *Common Criteria* is also undergoing review by ISO in anticipation of its subsequent release as an ISO Standard; the current *Common Criteria* release, version 2.0 Final, dated May 1998, has been accepted by ISO as ISO Final Draft International Standard 15408. CCT will incorporate new versions of the *Common Criteria* and *Common Methodology* as they evolve. New test methods also may be incorporated into CCT as they are developed and adopted.

NIAP, a partnership between NIST and NSA, requested the development of the CCT program to accredit laboratories that conduct IT security evaluations under the Common Criteria Scheme. The Common Criteria Scheme is the NIAP program to manage the evaluation and validation of IT security products using the *Common Criteria* and *Common Methodology*. IT security products validated by this program will receive a Common Criteria Certificate and be listed on the NIAP Validated Products List. Through a mutual recognition arrangement signed by the United States and the other *Common Criteria* sponsoring nations, these other countries will recognize products placed on the NIAP Validated Products List. For more information on NIAP and the Common Criteria Scheme, see Sec. 285.4 References.

Sec. 285.4 References

Reference documents, standards, and publications for NVLAP and NIAP are given below.

(a) NVLAP publications

(1) NIST Handbook 150, *NVLAP Procedures and General Requirements*

(2) NIST Special Publication 810, *NVLAP Directory* (most current edition)

NVLAP publications may be ordered from:

NVLAP
National Institute of Standards and Technology
100 Bureau Drive, Stop 2140
Gaithersburg, MD 20899-2140

Phone: (301) 975-4016
Fax: (301) 926-2884
e-mail: nvlap@nist.gov

NIST Handbook 150 and the On-line Directory of Accredited Laboratories are also available on the NVLAP website: http://ts.nist.gov/nvlap.

(b) NIAP publications

(1) *NIAP Common Criteria Evaluation and Validation Scheme for Information Technology Security: Organization, Management, and Concept of Operations (Scheme Publication #1)*

NIAP publications may be obtained from:

National Information Assurance Partnership
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899-8930
e-mail: niap-info@nist.gov

or obtained from the NIAP web site, http://niap.nist.gov/

(c) ISO Publications

(1) ISO/IEC Guide 25 - *General Requirements for the Competence of Calibration and Testing Laboratories*

(2) ISO/IEC Technical Report 13233, *Information Technology - Interpretation of Accreditation Requirements in ISO/IEC Guide 25 - Accreditation of Information Technology and Telecommunications Testing Laboratories for Software and Testing Services*

ISO publications may be ordered from:
ISO/IEC
Case Postale 56
CH-1211 Geneve 20
Switzerland

(d) Other Publications

(1) *Common Criteria for Information Technology Security Evaluation*

(2) *Common Methodology for Information Security Evaluation*

These publications may be obtained from the following websites:

http://www.radium.ncsc.mil/tpep/library/ccitse/
http://csrc.nist.gov/cc/

Sec. 285.5 Definitions

Common Criteria Certificate: Formal recognition by the NIAP Validation Body that the IT security evaluation has been conducted in accordance with the Common Criteria Scheme requirements using the *Common Criteria* and the *Common Methodology*. A product that has received a Common Criteria Certificate is placed on NIAP's Validated Products List.

Evaluation: The assessment of a Protection Profile, Security Target, or IT product against a set of *Common Criteria* requirements using the *Common Methodology*. This term is consistent with the NVLAP notion of "testing".

Evaluation Assurance Level (EAL): A package of *Common Criteria* assurance requirements that represents a point on the *Common Criteria* pre-defined assurance scale. At present, the *Common Criteria* defines seven hierarchical EALs, from EAL1 to EAL7; the higher EALs encompass the requirements of the lower EALs. CCT includes only EAL1 through EAL4 at this time.

IT Product: A package of IT software, firmware, and/or hardware, providing functionality designed for use or incorporation within a multiplicity of systems. An IT product can be a single product or multiple IT products configured as an IT system or system solution to meet certain consumer needs. In either case, the testing occurs in a testing facility or a client's site (under laboratory conditions) and not in the actual operational environments.

Key Technical Personnel: Laboratory personnel with the authority and responsibility to make the important technical evaluation decisions.

Protection Profile: An implementation-independent set of security requirements for a category of IT products that meet specific consumer needs.

Security Target: A set if security requirements and specifications to be used as the basis for evaluation under the *Common Criteria* of an identified Target of Evaluation (TOE). The security target specifies the security enforcing functions of the TOE. It also specifies the security objectives, the threats to those objectives, and any specific security mechanisms that are employed.

Target of Evaluation (TOE): An IT product and its associated administrator and user guidance documentation that is the subject of a security evaluation under the *Common Criteria*.

Test Method: An evaluation assurance package from the *Common Criteria* and the associated evaluation methodology for that assurance package from the *Common Methodology*.

Validation: The NIAP Validation Body's review of an IT security evaluation to determine if issuance of a *Common Criteria Certificate* is warranted.

Sec. 285.6 NVLAP documentation.

(a) Handbooks

(1) The NVLAP procedures and general requirements are contained in NIST Handbook 150. Handbook 150 is used for all NVLAP testing laboratory and calibration laboratory programs. The portions of Handbook 150 marked with a triangle in the margin do not apply to CCT laboratories; they concern calibration laboratories.

(2) The technical procedures, program-specific requirements, and interpretations for CCT are contained in this handbook.

(b) Checklists

(1) Checklists contain definitive questions about all aspects of the NVLAP criteria for accreditation. NVLAP programs incorporate two types of checklists: (1) a General Operations Checklist (Appendix B) and (2) a Specific Operations Checklist (Appendix C).

(2) Checklists are used by the NVLAP assessor(s) during the on-site assessment, discussed during the exit briefing, and signed by the laboratory representative and the assessor, and a copy is given to the laboratory. The checklists become part of the laboratory history kept by NVLAP.

(i) The NVLAP General Operations Checklist, based on section 285.33 of Handbook 150, is applicable to evaluating a laboratory's ability to conduct testing in general. It addresses factors such as the laboratory's organization, management, and quality system in addition to its testing competency. This checklist will be revised only when Handbook 150 is revised.

(ii) The Specific Operations Checklist is specific to CCT and focuses on IT security evaluation requirements and any special personnel and equipment requirements of Handbook 150-20. This checklist may be revised when appropriate to reflect changes in the technical requirements, scope, and/or technology of the program.

(3) Each of the two checklists ends with a Comments and Deficiencies form. The assessor uses these forms to explicitly identify and describe deficiencies noted in the body of the checklist. Additionally, the assessor may use the form to document comments on any aspect of the laboratory or its performance.

(c) Test Method Selection List

Most NVLAP programs have scopes that cover more than one test method. Depending on the breadth of its testing capabilities, a laboratory may seek accreditation to all or only selected methods within the scope of the program. In such cases, the methods are given on the Test Method Selection List, which is provided to a laboratory seeking accreditation as part of the NVLAP application package for the program.

Appendix D shows the Test Method Selection List for CCT. At present, the test methods comprise the evaluator actions from the *Common Criteria* and the associated *Common Methodology* for the security evaluation of Protection Profiles, Security Targets, and Targets of Evaluation (TOEs) at assurance levels EAL1 through EAL4. Because the EALs are hierarchical and include the requirements of the lower EAL, accreditation at a particular EAL means the laboratory meets the requirements and is accredited to conduct evaluations at that EAL and each lower EAL. For instance, a laboratory accredited against the EAL3

test method can conduct EAL3, EAL2, and EAL1 evaluations.

Sec. 285.22 Assessing and evaluating a laboratory

This section discusses the assessing and evaluating of a laboratory for CCT. The section numbering is patterned after Handbook 150, but the assessment usually proceeds in the following sequence. First, the laboratory sends an application for accreditation and provides a copy of its quality manual to NVLAP. The NVLAP assessors will review the manual before conducting the on-site assessment and will review it with the laboratory during the on-site assessment. After a successful review of the quality manual, NVLAP will send the necessary materials for conduct of the proficiency testing to the laboratory, and the laboratory will respond with written answers and evaluation results. The proficiency test will be reviewed by IT security evaluation technical experts and the results of the proficiency test will be reviewed with the laboratory during the on-site assessment. After successful completion of proficiency testing, the on-site assessment is conducted, and the laboratory is provided with the results of the assessment. After all assessment activities have concluded, an evaluation is made of all results and an accreditation decision is made by NVLAP.

(a) On-Site Assessment

(1) The on-site assessment will be arranged with the laboratory after the laboratory quality manual has been reviewed by the assessors. If the quality manual does not appear to meet CCT requirements, the assessor may request additional information before the on-site assessment is scheduled.

(2) The on-site assessment will be performed by two or more NVLAP assessors during a two and a half day period. The assessment will take place at the laboratory site. All observations made by the assessors during the assessment will be held in strict confidence.

The laboratory shall have its facilities and equipment in good working order and be ready for examination according to the requirements identified in this handbook, NIST Handbook 150, and the laboratory's quality manual. Efforts will be made to minimize disruption to the normal working routines during the assessment. The assessors will need time and work space to complete assessment documentation during their time at the laboratory site.

The assessors will use the NVLAP General Operations Checklist and the CCT-Specific Operations Checklist. The checklists, based on Handbook 150 and the technical specifics contained in this handbook, ensure that the assessment is complete and that all assessors cover the same items at each laboratory. The assessors may request additional information in an effort to clarify checklist responses or to delve more deeply into a technical issue.

(3) The agenda for a typical on-site assessment is given below.

(i) The assessors meet with laboratory management and supervisory personnel to explain the purpose of the on-site assessment and to discuss the schedule for the assessment activities. Information provided by the laboratory on its application form may be discussed during this meeting. At the discretion of the laboratory manager, other staff may attend this meeting.

The assessors will ask the laboratory manager to assist in arranging times for interviews with laboratory staff members. While it is not necessary for the assessors to talk to all staff members, they may select staff members representing all aspects of the laboratory. Assessors will also talk to staff members who have participated in proficiency testing.

Laboratory personnel should not be nervous answering assessor questions and should not answer any question they feel unqualified to answer. Knowing whom to ask or where to find the answer is usually considered an acceptable response by the assessors.

(ii) The assessors review laboratory documentation, including the quality system, quality manual, equipment and maintenance records, software versions, record keeping procedures, testing procedures, laboratory evaluation records and reports, personnel competency records, personnel training plans and records, procedures for updating pertinent information (e.g., *Common Criteria* or *Common Methodology* versions, NIAP Validation Body guidance or

interpretations, or the validated products list), and safeguards for the protection of vendor-sensitive and proprietary information.

The assessors will have reviewed the quality manual submitted to NVLAP before the on-site assessment. The assessors will discuss the manual with the designated laboratory staff.

One (or more) laboratory staff member(s) must be available to answer questions; however, the assessors may wish to review the documents without laboratory staff present. The assessors do not usually ask to remove any documents from the laboratory site.

The assessors will check personnel information for job descriptions, resumes, and technical performance reviews. The assessors need not be given information that violates individual privacy such as salary, medical information, or performance reviews outside the scope of the laboratory's accreditation. At the discretion of the laboratory, a member of its Human Resources Department may be present during the review of personnel information.

(iii) The assessors will discuss the results of the proficiency test with individuals or team members who have participated in the tests. Answers and rationale may be discussed, and some aspects of the tests may be expanded or explained during these discussions. Records that have been generated during proficiency testing will be audited.

(iv) At the end of the on-site assessment, an exit briefing is held with the laboratory manager and staff to discuss the assessors' findings. Deficiencies are discussed and resolutions may be mutually agreed upon. Items that must be addressed before accreditation can be granted are emphasized, and outstanding deficiencies require subsequent response to NVLAP within 30 days. Items that have been corrected during the on-site assessment and any recommendations are specifically noted.

Comments not identified as deficiencies by the assessors should be given serious consideration by the laboratory. However, any resulting actions are taken at the laboratory's discretion. Any disagreements between the laboratory and the assessors should be referred to NVLAP for further evaluation.

(v) The assessors complete an on-site assessment report, which summarizes the findings. The assessors attach copies of the completed checklists to this report during the exit briefing. The report and the checklists are signed by the assessors and the laboratory's Authorized Representative. A copy of the report and checklists is given to the laboratory representative for retention.

(b) Proficiency Testing

(1) Applicant laboratories are required to participate satisfactorily in proficiency testing for identified test methods. NIST Handbook 150 describes how proficiency testing is included in the accreditation process. Proficiency testing is generally required prior to initial accreditation and periodically thereafter. Laboratories renewing accreditation must have satisfactorily participated in all required proficiency testing during their previous accreditation period. Proficiency testing is required for CCT as designated in the Test Method Selection List (Appendix D).

To evaluate the effective and proper operation of a laboratory, proficiency testing may consist of several parts. The proficiency test concept is designed to allow the evaluation of the laboratory's ability to produce repeatable and reproducible evaluation results.

For CCT, proficiency testing will assess both the laboratory's academic and applied competence in the conduct of security evaluations. The following methods will be used to assess laboratory proficiency:

(i) Academic knowledge and understanding of the concepts and criteria underlying IT security evaluations will be assessed with a written quiz to be taken by laboratory personnel. The quiz is intended to establish laboratory competence in areas germane to the conduct of security evaluations. The quiz will pose questions in areas such as IT security, *Common*

Criteria, and *Common Methodology*. The questions will correspond to the test method(s) (e.g., EAL3 and corresponding methodology) for which the laboratory is seeking accreditation.

(ii) Applied competence will be assessed with evaluation exercises using artifacts provided by NVLAP and applying the test method(s) for which the laboratory is seeking accreditation. The laboratory will produce part, or all, of an evaluation report, documenting the security evaluation results. The evaluation exercises are intended to assess the laboratory's competence in conducting security evaluations, not to evaluate all artifacts in their entirety. As such, the exercises will be focused and bounded, and the artifact may or may not be compliant with the *Common Criteria*.

Upon receipt by NVLAP of the laboratory's application for accreditation, and after a preliminary review of the laboratory's quality system documentation, of the necessary materials for the conduct of the proficiency testing will be provided to the laboratory. Instructions will also be provided. The laboratory will be required to respond with written answers and evaluation results prior to the on-site assessment.

The proficiency tests may be taken by individuals or by a team. The individuals or team members will be selected by the laboratory management. All individuals or team members who participate in the proficiency tests must sign the written quiz and the security evaluation report.

The laboratory will be required to agree not to disclose the proficiency tests or results outside of the laboratory and shall have procedures in place to ensure that the confidentiality and integrity of the proficiency tests are preserved.

(2) The results of proficiency testing will be reported to the participants in appropriate documents and reports. Problems indicated by proficiency testing will be discussed with appropriate laboratory personnel responsible for developing and implementing plans for resolving the problems.

Proficiency tests will be used as a vehicle for discussion during the on-site assessment with individuals or team members who have participated in the tests. Answers and rationale may be discussed, and some aspects of the tests may be expanded or explained during these discussions. It is expected that the laboratory will be following its documented system quality procedures during the conduct of the proficiency tests. Records that have been generated during the security evaluation exercises will be audited during the on-site assessment.

Deficiencies identified by proficiency testing, scheduled proficiency testing, or submission of an evaluation report must be resolved in a manner similar to the process for on-site assessment deficiency resolution.

(3) It is anticipated that, after initial accreditation, proficiency testing will be conducted at two-year intervals, in the year when there is no on-site assessment.

Sec. 285.23 Granting and renewing accreditation

Two documents are issued to laboratories that have been granted NVLAP accreditation: a Certificate of Accreditation and a Scope of Accreditation. Samples of these accreditation documents for CCT are shown in Appendix A.

Laboratories are granted accreditation for a period of one year, renewable annually. The on-site assessment portion of the accreditation process will occur every two years unless additional observation becomes necessary.

Sec. 285.24 Denying, suspending, and revoking accreditation

Failure to comply with all NVLAP requirements, as specified in this Handbook and in NIST Handbook 150, *NVLAP Procedures and General Requirements*, may result in the denial, suspension, or revocation of a laboratory's accreditation. This includes failure to resolve noted deficiencies and failure to successfully participate in proficiency testing activities.

Sec. 285.33 Criteria for accreditation

(a) Scope

This section presents the specific requirements for a laboratory to demonstrate that it is competent to conduct IT security evaluations using the *Common Criteria* and the *Common Methodology*.

(b) Organization and management

The laboratory shall establish and maintain policies and procedures for maintaining laboratory impartiality and integrity in the conduct of IT security evaluations. The laboratory shall:

- ensure that its personnel are free from any commercial, financial, or other pressures that might adversely affect the impartiality of their work, and

- be organized in such a way that confidence in its independence of judgment and integrity is maintained at all times.

For laboratories conducting evaluations under the Common Criteria Scheme, this means:

- the same laboratory member or team cannot develop and evaluate the same Protection Profile, Security Target, or IT product, and

- the same laboratory member cannot provide consulting services for and then participate in the evaluation of the same Protection Profile, Security Target, or IT product.

To support this, the laboratory shall have an explicit policy and set of procedures for maintaining separation, both physical and electronic, between the laboratory evaluators and product developers, system integrators, and others who may have an interest in and may unduly influence the evaluation outcome. The laboratory shall have procedures that support effective communication within the laboratory, between the laboratory and its customers (e.g., vendors, sponsors, and the NIAP Validation Body), and with the general public.

(c) Quality system, audit and review

(1) The quality system requirements are designed to promote laboratory practices that ensure technical accuracy and integrity of the security evaluation and adherence to quality assurance practices appropriate to CCT. The laboratory must maintain a quality system that fully documents the laboratory's policies, practices, and the specific steps taken to ensure the quality of the IT security evaluations.

The quality system must provide for periodic reviews of the competence of the staff involved in the conduct of security evaluations.

The reference documents, standards, and publications listed in Sec. 285.4 of this handbook shall be available as references in developing and maintaining the quality system and for use by laboratory staff.

Records must be kept of all quality system activities.

The laboratory shall establish and maintain documented procedures for the review of contracts between itself and its clients. The contract review shall be conducted to ensure that the laboratory is capable of providing the service and that the requirements, rights, and responsibilities of the parties are understood.

(2) The quality manual must contain, or refer to, documentation that describes and details the laboratory's implementation of procedures covering all of the technical requirements in this handbook and NIST Handbook 150. This information will be reviewed by NVLAP assessors during on-site assessments.

The quality manual must include, or refer to, policies and procedures to ensure the protection of proprietary information. This protection must specify how proprietary information will be protected from personnel outside the laboratory, from visitors to the laboratory, from laboratory personnel without a need to know, and from other unauthorized persons. These policies and procedures will be subject to audit by NVLAP.

The quality manual must include procedures for software handling and integrity, and additional procedures for conducting security evaluation at client sites, if applicable. For example, client site procedures may explain how to secure the site, where to store records and documentation, and how to control access to the test facility.

(3) Audits and management reviews must be conducted on a periodic basis.

(i) In the case where only one member of the laboratory staff is competent to conduct a specific aspect of a test method, internal audits may be conducted of the process and may include a review of documented procedures and instructions, adherence to procedures and instructions, and review of previous audit reports.

(ii) In order to audit technical aspects of the program, external audits by NVLAP or another appropriate organization, submission of evaluation reports to the NIAP Validation Body, and/or telephone audits by Technical Experts may be used.

(d) Personnel

(1) The laboratory shall maintain a competent administrative and technical staff appropriate for *Common Criteria* based IT security evaluations. The laboratory shall maintain position descriptions and resumes for the laboratory staff members who conduct security evaluations and responsible supervisory personnel.

The laboratory shall maintain a list of personnel designated to fulfill NVLAP requirements including: laboratory director, authorized representative, approved signatories, and key technical personnel. The laboratory must also identify a staff member as quality manager who has overall responsibility for the quality system and maintenance of the quality manual. An individual may be assigned or appointed to serve in more than one position; however, to the extent possible, the laboratory director and the quality manager positions should be independently staffed.

(2) Laboratories shall document the required qualifications for each staff position involved in the IT security evaluation process. The staff information may be kept in the official personnel folders or in separate, official folders that contain only the information that the NVLAP assessors need to review.

(3) Laboratory staff members who conduct IT security evaluation activities shall have a Bachelor of Science in Computer Science, Computer Engineering, or related technical discipline or equivalent experience.

Laboratory staff collectively shall have knowledge or experience in the following areas: operating systems, data structures, design/analysis of algorithms, database systems, programming languages, computer systems architectures, and networking.

Training for the laboratory staff shall concentrate on the following areas:

(i) general requirements of the test methods including generation of evaluation reports;

(ii) computer science concepts;

(iii) computer security concepts;

(iv) working knowledge of the *Common Criteria*; and

(v) working knowledge of the *Common Methodology*.

(4) The laboratory shall have a detailed documented description of its training program for new and current staff members. Each new staff member must be trained for assigned duties. The training program must be updated and current staff members must be retrained when the *Common Criteria*, *Common Methodology*, or scope of accreditation changes, or when the individuals are assigned new responsibilities. Each staff member may receive training for assigned duties either through on-the-job training, formal classroom study, or another appropriate mechanism. Training materials that are maintained within the laboratory must be kept up-to-date.

(5) The laboratory shall review the competence of each staff member for each test method the staff member is authorized to conduct. The immediate supervisor, or a designee appointed by the laboratory director, must conduct annually an assessment and an observation of performance for each staff member. A record of the annual review of each staff member must be dated and signed by the supervisor and the employee.

A description of competency review programs shall be maintained in the quality manual.

(e) Accommodation and environment

(1) The laboratory shall have adequate facilities to conduct IT security evaluations. This includes facilities for security evaluation, staff training, record keeping, document storage, and software storage.

(2) A proprietary protection system must be in place to safeguard client proprietary hardware, software, test data, electronic and paper records, and other materials. This system must protect the

proprietary materials and information from personnel outside the laboratory, visitors to the laboratory, laboratory personnel without a need to know, and other unauthorized persons. Laboratory networks used to conduct IT security evaluations must also be isolated from those outside the laboratory.

(3) Electronic mail capability is required for communications with the NIAP Validation Body. Internet access also is required for obtaining revisions to the *Common Criteria*, *Common Methodology*, guidance, and interpretations. In addition, laboratories must have an effective virus protection and software/data backup program.

(4) If the laboratory is conducting its evaluation at the client site or other location outside the laboratory facility, the environment still must conform to the requirements levied on a laboratory environment. If a client's system on which evaluation is conducted is potentially open to access by unauthorized entities during evaluation, the evaluation laboratory shall control the evaluation environment in such a way that unauthorized entities do not gain access to that system during evaluation.

(5) If the laboratory is conducting multiple simultaneous evaluations, it must maintain a system of separation between the products of different clients and evaluations, to include the product under evaluation, the test platform, peripherals, and documentation.

(f) Equipment and reference materials

(1) The laboratory must maintain on-site systems adequate to support IT security evaluations in keeping with the test methods for which it is seeking accreditation. The laboratory also must have an electronic report generation capability.

(2) The laboratory must document and maintain records on all test equipment or test suites within its control, to include customer-supplied equipment and laboratory-supplied equipment. The laboratory must also know how to configure and operate all equipment within its control.

(g) Measurement traceability and calibration

(1) The equipment used for conducting security evaluations must be maintained:

(i) in accordance with the manufacturer's recommendations, or

(ii) in accordance with internally documented laboratory procedures, as applicable.

Neither the Common Criteria Scheme nor the NVLAP mandates the use of any particular evaluation equipment; therefore, these requirements may not be applicable. "Test equipment" may refer, however, to software evaluation tools or other assessment mechanisms used by the laboratory to evaluate the security of an IT product.

(2) Laboratories must *calibrate* their test equipment. In CCT, *calibration* means *verification of correctness*. Any test tools used to conduct security evaluations that are not part of the unit under evaluation need to be studied in isolation to make sure they correctly represent and assess the test assertions they make. They must also be examined to ensure they do not interfere with the conduct of the test and do not modify or impact the integrity of the product under test in any way.

(3) The reference standards used and the environmental conditions at the time of calibration must be documented for all calibrations. Calibration records and evidence of the traceability of the reference standards used must be made available for inspection during the on-site visit.

(4) For CCT, "traceability to national standards of measurement" is interpreted to mean that security evaluation activities must be traceable to the evaluator actions in the *Common Criteria* and the *Common Methodology*. This means that test tools must demonstrate that the tests they conduct and the test assertions they make are traceable to the criteria and methodology. This is necessary to ensure that test results constitute credible evidence of compliance with the criteria and methodology.

(h) Calibration and test methods

(1) For the purposes of achieving product validation through the Common Criteria Scheme, laboratories must comply with NIAP-specified guidance and interpretations of the evaluation criteria. The NIAP Validation Body may issue

technology guidance or interpretations to supplement the evaluation assurance criteria or methodology provided in the *Common Criteria* and *Common Methodology*; the laboratory shall comply with the guidance or interpretations within the timeframe specified by the NIAP Validation Body.

The laboratory shall have documented procedures for conducting security evaluations using the *Common Criteria* and *Common Methodology*, and for complying with guidance or interpretations. The laboratory shall ensure that these procedures are being followed.

The *Common Criteria*, *Common Methodology*, NIAP Validation Body guidance and interpretations, and the laboratory's procedures for conducting security evaluations shall be maintained up-to-date and be readily available to the staff.

(2) Security evaluations may be conducted at the client or laboratory site or other mutually agreed upon site. When evaluation is conducted at a client site, only the laboratory personnel shall perform all actions necessary to conduct the tests and record the results.

(3) If the laboratory conducts security evaluations at a site other than the laboratory site, it must have additional procedures in place to ensure that the same requirements beholden to the laboratory and its facility are maintained at the non-laboratory site.

(4) The test methods, as defined by NIAP, are contained in Appendix D. At present, the test methods include *Common Criteria* APE and ASE Assurance Classes, and EALs 1-4 along with the corresponding *Common Methodology* methodology. While the current scope of accreditation for EALs 1-4 is limited to IT products, it may be expanded in the future to include system evaluations.

(5) When exceptions to the evaluation methodology are deemed necessary for technical reasons, the client shall be informed and details shall be described in the evaluation report.

(i) Handling of calibration and test items

(1) The laboratory must protect products under evaluation and calibrated tools from modification, unauthorized access, and use. The laboratory must also maintain separation between and control over the items from different evaluations, to include the product under evaluation, its platform, peripherals, and documentation.

(2) When the product under evaluation consists of software components, the laboratory shall ensure that configuration management mechanisms are in place to prevent inadvertent modifications to the software components during the evaluation process.

(j) Records

(1) The laboratory shall maintain a functional record-keeping system for each security evaluation. Records must be easily accessible and contain complete information on the evaluation. Records of evaluation activities must be traceable to *Common Criteria* evaluator actions and *Common Methodology* work units. Computer-based media must be logged and properly marked, and there must be proper back-up. Entries in laboratory notebooks must be dated and signed or initialed. Computer-based records must contain entries of pertinent staff/date information as required in the quality manual, as well as be maintained in accordance with laboratory guidelines and in a manner that ensures record integrity preservation. All laboratory records must be maintained, released, or destroyed in accordance with the laboratory's proprietary information policy and contractual agreements with clients. Laboratory records must be retained for a period of at least five years.

The laboratory must have a policy and set of procedures for ensuring the accuracy and integrity of its records. The laboratory shall take steps to ensure that no unauthorized entity can gain access to the physical and on-line records either during or after the evaluation.

(2) Records covering the following are required and will be reviewed during the on-site assessment by selective sampling:

(i) quality system;

(ii) staff training dates and competency reviews;

(iii) NVLAP proficiency test dates and results;

(iv) software versions and updates;

(v) statement of policy and conditions for evaluation;

(vi) evaluation methods and procedures;

(vii) acceptance/rejection of products submitted for evaluation;

(viii) comprehensive logs for tracking samples and evaluation activities;

(ix) evaluation data (including any diagrams, photos, and graphic images) and official reports;

(x) calibration of test tools and equipment;

(xi) audits and management reviews;

(xii) test files;

(xiii) equipment.

(3) Evaluation equipment, test tools and equipment, and calibration records should include the following:

(i) equipment name or description;

(ii) model, style, or serial number;

(iii) manufacturer;

(iv) notation of all equipment variables requiring calibration;

(v) the range of calibration;

(vi) the resolution of the instrument and its allowable error;

(vii) calibration date and schedule;

(viii) date and result of last calibration;

(ix) identity of the laboratory individual or external service responsible for calibration; and

(x) source of reference standard and traceability.

(k) Certificates and reports

(1) The laboratory shall issue evaluation reports of its work that accurately, clearly, and unambiguously present the evaluation conditions, evaluation setup, evaluation results, and all required information. Evaluation reports to clients should meet contractual requirements. Evaluation reports should provide all necessary information to permit the same or another laboratory to repeat the evaluation and obtain comparable results. The laboratory shall provide evidence to support the results of the IT security evaluations.

Comments and results that are outside the scope of the test methods for which the laboratory is accredited must be marked as such.

(2) There are two types of evaluation reports:

(i) reports that are produced under contract and intended for use by the client; and

(ii) reports that are to be submitted to the NIAP Validation Body.

Reports intended for use only by the client shall meet client/laboratory contract obligations and be complete, but need not necessarily meet all NIAP requirements. The evaluation report must contain sufficient information for the exact test conditions to be reproduced at a later time if a retest is necessary.

Evaluation reports created for submission to the NIAP Validation Body must meet the requirements of the Common Criteria Scheme. Evaluation reports shall be submitted in the form and by the method specified.

In addition to printed reports, laboratories may submit reports to the NIAP Validation Body in electronic form using media such as floppy disks. The electronic version shall have the same content as the hardcopy version using an application (e.g., WordPerfect or Microsoft Word) that is acceptable to the NIAP Validation Body.

(3) Evaluation reports that will be delivered to the NIAP Validation Body in electronic form via electronic transfer technology shall be digitally signed or have a message authentication code applied to ensure integrity of the report and the identity of the laboratory that produced the report. The laboratory shall provide a secure means of conveying the necessary information to the NIAP Validation Body for the verification of the signature or the message authentication code. Confidentiality mechanisms shall be employed to ensure that the evaluation report cannot be disclosed to anyone other than the intended recipient(s).

(4) Changes to evaluation reports produced for the NIAP Validation Body must be done in accordance with NIAP requirements. For evaluation reports produced for purposes other than validation, the laboratory shall issue corrections or additions to an evaluation report only by a further document suitably marked; e.g., "Supplement to evaluation report serial number ..." If the change involves a *Common Criteria* requirement, this document must specify which *Common Criteria* requirement is in question, the content of the result, the explanation of the result, and the reason for acceptance of the result.

APPENDIX A

SAMPLE ACCREDITATION DOCUMENTS

The sample Scope of Accreditation and Certificate of Accreditation
will be available in future releases of this document.

APPENDIX B

GENERAL OPERATIONS CHECKLIST

GENERAL OPERATIONS CHECKLIST

Instructions to the Assessor: This checklist addresses general accreditation criteria prescribed in applicable sections of NIST Handbook 150, *NVLAP Procedures and General Requirements*.

This checklist follows and is numbered to correspond to the *NVLAP Procedures and General Requirements*, Subsection 285.33. The numbers in square brackets identify related checklist items. A small black triangle appears in the left-hand margin of selected lines of text throughout this checklist; the marked text applies only to the Calibration Laboratory Accreditation Program (LAP).

Place an "X" beside each checklist item which represents a deficiency. Place a "C" beside each item on which you are commenting for other reasons. Record the item number and your written deficiency explanations and/or comments in this list or on the attached comment sheets. Place a check beside all other items you observed or verified at the laboratory.

SEC. 285.33 CRITERIA FOR ACCREDITATION

(b) *Organization and management*

(1) The laboratory shall be:

_____ (i) legally identifiable;

Legal name of laboratory ownership: _____

_____ (ii) organized and shall operate in such a way that its permanent, temporary and mobile facilities meet the NVLAP requirements [see also (b)(2)(i), (c)(2)(ii)];

_____ (iii) properly identified on the NVLAP Application.

(2) The laboratory shall:

_____ (i) have managerial staff with the authority and resources needed to discharge their duties [see also (b)(1)(ii), (c)(2)(ii)];

_____ (ii) have policies to ensure that its personnel are free from any commercial, financial and other pressures which might adversely affect the quality of their work;

_____ (iii) be organized in such a way that confidence in its independence of judgment and integrity is maintained at all times;

_____ (iv) specify and document the responsibility, authority and interrelation of all personnel who manage, perform or verify work affecting the quality of calibrations and tests;

_____ (v) provide supervision by persons familiar with the calibration or test methods and procedures, the objective of the calibration or test, and the assessment of the results. The ratio of supervisory to non-supervisory personnel shall be such as to ensure adequate supervision;

_____ (vi) have a technical manager (however named) who has overall responsibility for the technical operations;

Name of person: _____

_____ (vii) have a quality manager (however named) who has responsibility for the quality system and its implementation. The quality manager shall have direct access to the highest level of management at which decisions are taken on laboratory policy or resources, and to the technical manager. In some laboratories, the quality manager may also be the technical manager or deputy technical manager;

Name of person: _____

_____ (viii) nominate deputy(ies) in case of absence of the technical or quality manager;

Name(s): _____

_____ (ix) have documented policy and procedures to ensure the protection of clients' confidential information and proprietary rights [see also (c)(2)(xviii)];

_____ (x) where appropriate, participate in interlaboratory comparisons and proficiency testing programs [see also (c)(2)(xiv), (c)(6)(ii), (g)(3)];

_____ (xi) have documented policy and procedures to ensure that its clients are served with impartiality and integrity.

(c) ***Quality system, audit and review***

(1) The laboratory shall:

_____ (i) have an established and maintained quality system appropriate to the type, range and volume of calibration and testing activities it undertakes;

_____ (ii) have the elements of the quality system documented;

_____ (iii) ensure that the quality documentation is available for use by the laboratory personnel;

_____ (iv) define and document its policies and objectives for, and its commitment to, good laboratory practice and quality of calibration or testing services;

_____ (v) have the laboratory management which ensures that these policies and objectives are documented in a quality manual and communicated to, understood, and implemented by all laboratory personnel concerned;

_____ (vi) ensure that the quality manual is maintained current under the responsibility of the quality manager [see also (c)(2)(iv)].

Date of quality manual: _____

Date of latest update: _____

_____ (2) The quality manual, and related quality documentation, shall state the laboratory's policies and operational procedures established in order to meet the NVLAP requirements. The quality manual and related quality documentation shall contain:

_____ (i) a quality policy statement, including objectives and commitments, by top management;

_____ (ii) the organization and management structure of the laboratory, its place in any parent organization and relevant organizational charts;

_____ (iii) the relations between management, technical operations, support services and the quality system;

_____ (iv) procedures for control and maintenance of documentation [see also (c)(1)(vi), (j)(1)];

_____ (v) job descriptions of key staff and reference to the job descriptions of other staff;

_____ (vi) identification of the laboratory's approved signatories (list here or in the comments section): _____

_____

_____ (vii) the laboratory's procedures for achieving traceability of measurements;

_____ (viii) the laboratory's scope of calibrations and/or tests;

_____ (ix) written procedures for ensuring that the laboratory reviews all new work to ensure that it has the appropriate facilities and resources before commencing such work;

_____ (x) reference to the calibration, verification and/or test procedures used;

_____ (xi) procedures for handling calibration and test items;

_____ (xii) reference to the major equipment and reference measurement standards used;

_____ (xiii) reference to procedures for calibration, verification and maintenance of equipment;

_____ (xiv) reference to verification practices including interlaboratory comparisons, proficiency testing programs, use of reference materials and internal quality control schemes [see also (b)(2)(x), (c)(6)(ii), (g)(3)];

_____ (xv) procedures to be followed for feedback and corrective action whenever:

_____ a) testing discrepancies are detected, or

_____ b) departures from documented policies and procedures occur;

_____ (xvi) the laboratory management policies for departures from documented policies and procedures or from standard specifications;

_____ (xvii) procedures for dealing with complaints [see also (n)];

_____ (xviii) procedures for protecting confidentiality and proprietary rights [see also (b)(2)(ix)];

_____ (xix) procedures for audit and review;

_____ (xx) a description of the laboratory's policy regarding the use of the NVLAP logo;

_____ (xxi) a statement of the laboratory's policy for establishing and changing calibration intervals for equipment it controls; and

_____ (xxii) a statement of the laboratory's policy concerning the technique(s) to be used for determining measurement uncertainty and calibration/verification adequacy.

_____ (3) The laboratory shall arrange for audits of its activities at appropriate intervals to verify that its operations continue to comply with the requirements of the quality system. Such audits shall be carried out by trained and qualified staff who are, wherever possible, independent of the activity to be audited. Where the audit findings cast doubt on the correctness or validity of the laboratory's calibration or test results, the laboratory shall take immediate corrective action and shall immediately notify, in writing, any client whose work may have been affected.

The audits shall be objective and be conducted internally or on contract. The audits shall include both general criteria (documents, records and policies) and technical compliance (test methods and practices and calibration procedures).

_____ (4) The quality system adopted to satisfy the NVLAP requirements shall be reviewed at least once a year by the management to ensure its continuing suitability and effectiveness and to introduce any necessary changes or improvements.

_____ (5) All audit and review findings and any corrective actions that arise from them shall be documented. The person responsible for quality shall ensure that these actions are discharged within the agreed timescale.

(6) In addition to periodic audits the laboratory shall ensure the quality of results provided to clients by implementing checks. These checks shall be reviewed and shall include, as appropriate, but not be limited to:

_____ (i) internal quality control plans, such as control charts and other available statistical techniques;

NOTE: Measurement assurance techniques are acceptable means to control the measurement process and consistently produce the highest quality measurements.

_____ (ii) participation in proficiency testing or other interlaboratory comparisons [see also (b)(2)(x), (c)(2)(xiv), (g)(3)];

_____ (iii) regular use of certified reference materials and/or in-house quality control using secondary reference materials;

_____ (iv) replicate testings using the same or different methods;

_____ (v) retesting of retained items;

_____ (vi) correlation of results for different characteristics of an item.

(d) *Personnel* [see also (c)(2)(v)]

_____ (1) The testing laboratory shall have sufficient personnel, having the necessary education, training, technical knowledge and experience for their assigned functions.

_____ (2) The testing laboratory shall ensure that the training of its personnel is kept up-to-date.

_____ (3) Records on the relevant qualifications, training, skills and experience of the technical personnel shall be maintained by the laboratory.

(e) ***Accommodation (facilities) and environment*** [see also (i)(3)]

_____ (1) Laboratory accommodation, calibration and test areas, energy sources, lighting, heating and ventilation shall be such as to facilitate proper performance of calibrations or tests.

NOTE: Laboratory design will be, to the maximum extent practical, in accordance with the guidelines found in the NCSL Recommended Practice #7, *Laboratory Design*, July 25, 1993.

_____ (2) The environment in which these activities are undertaken shall not invalidate the results or adversely affect the required accuracy of measurement. Particular care shall be taken when such activities are undertaken at sites other than the permanent laboratory premises.

NOTE: It is expected that environments which do not meet generally accepted norms, such as those found in NCSL Recommended Practice #7, yet which exhibit the stability required to apply necessary correction factors, will be specified by the laboratory for the purpose of assessment of compliance with its own procedures to achieve its stated uncertainties.

_____ (3) The laboratory shall provide facilities for the effective monitoring, control and recording of environmental conditions as appropriate. Due attention shall be paid, for example, to biological sterility, dust, electromagnetic interference, humidity, voltage, temperature, and sound and vibration levels, as appropriate to the calibrations or tests concerned.

_____ (4) There shall be effective separation between neighboring areas when the activities therein are incompatible.

_____ (5) Access to and use of all areas affecting the quality of these activities shall be defined and controlled.

_____ (6) Adequate measures shall be taken to ensure good housekeeping in the laboratory.

NOTE: While it is the laboratory's responsibility to comply with relevant health and safety requirements, this is outside the scope of this assessment.

(f) ***Equipment and reference materials***

(1) The laboratory shall:

_____ (i) be furnished with all items of equipment (including hardware, software, and reference materials) required for the correct performance of calibrations and tests;

_____ (ii) in those cases where the laboratory needs to use equipment outside its permanent control, including rented, leased and client-owned equipment, ensure that the relevant NVLAP requirements are met.

_____ (2) All equipment shall be properly maintained. Maintenance procedures shall be documented. Any item of the equipment which has been subjected to overloading or mishandling, or which gives suspect results, or has been shown by verification or otherwise to be defective, shall be taken out of service, clearly identified and wherever possible stored at a specified place until it has been repaired and shown by calibration, verification or test to perform satisfactorily. The laboratory shall examine the effect of this defect on previous calibrations or tests.

_____ (3) Each item of equipment including reference materials shall, when appropriate, be labeled, marked or otherwise identified to indicate its calibration status.

_____ (4) Records shall be maintained of each item of equipment and all reference materials significant to the calibrations or tests performed. The records shall include:

_____ (i) the name of the item of equipment, software or reference material;

_____ (ii) the manufacturer's name, type identification, and serial number or other unique identification;

_____ (iii) date received and date placed in service;

NOTE: For initial accreditation, the date received and the date placed in service are not considered mandatory requirements for inclusion in laboratory records, although this is encouraged as good laboratory practice.

_____ (iv) current location, where appropriate;

_____ (v) condition when received (e.g., new, used, reconditioned);

_____ (vi) copy of the manufacturer's instructions, where available;

_____ (vii) dates and results of calibrations and/or verifications and date of next calibration and/or verification;

_____ (viii) details of maintenance carried out to date and planned for the future;

_____ (ix) history of any damage, malfunction, modification or repair;

_____ (x) measured value observed for each parameter found to be out of tolerance during calibration/verification.

(g) ***Measurement traceability and calibration***

_____ (1) All measuring and testing equipment having an effect on the accuracy or validity of calibrations or tests shall be calibrated and/or verified before being put into service. The laboratory shall have an established program for the calibration and verification of its measuring and test equipment. The program will ensure the recall or removal from service of any standard or equipment which has exceeded its calibration interval or is otherwise judged to be unreliable.

_____ (2) The overall program of calibration and/or verification and validation of equipment shall be designed and operated so as to ensure that, wherever applicable, measurements made by the laboratory are traceable to national standards of measurement where available. Calibration certificates shall, wherever applicable, indicate the traceability to national standards of measurement and shall provide the measurement results and associated uncertainty of measurement and/or a statement of compliance with an identified metrological specification.

NOTE: Traceability to national standards includes traceability to standards maintained or defined at national laboratories in foreign countries where applicable. In these cases, traceability is achieved via international standards. This includes intrinsic standards of measurement where available.

Where applicable, the methodology of the *Guide to the expression of uncertainty in measurement*: 1993, shall be used as the basis for expression of uncertainty of the measurement. NIST Technical Note 1297; January 1993, *Guidelines for Evaluating and Expressing the Uncertainty of NIST Measurement Results*, is a practical application document written around the *Guide to the expression of uncertainty in measurement*. Where detailed procedures are not used to quantify and combine uncertainties (i.e., use of test accuracy ratio concepts), the sources of uncertainty shall be tabulated and demonstrated to be acceptable for the measurement undertaken.

NOTE: A significant number of intrinsic standards, such as the Josephson Array Voltage Standard and the Iodine-Stabilized Helium-Neon Laser Length Standard, have been developed and are now being used by many national standards laboratories and some industrial laboratories. These standards are based on well-characterized laws of physics, fundamental constants of nature, or invariant properties of materials, and make ideal stable, precise, and accurate measurement standards if properly designed, characterized, operated, monitored and maintained. Where intrinsic standards are used, the laboratory should demonstrate by measurement assurance techniques, interlaboratory comparisons, or other suitable means, that its intrinsic standard measurement results are correlated with those of national or international standards.

_____ (3) Where traceability to national standards of measurement is not applicable, the laboratory shall provide satisfactory evidence of correlation of results, for example by participation in a suitable program of interlaboratory comparisons or proficiency testing [see also (b)(2)(x), (c)(2)(xiv), (c)(6)(ii)].

NOTE: Traceability requirements may also be satisfied by:

(i) internationally accepted standards in the field concerned;

(ii) suitable reference materials;

(iii) ratio or reciprocity measurements; or

(iv) mutual consent standards which are clearly specified and mutually agreed upon by all parties concerned.

_____ (4) Reference standards of measurement held by the laboratory shall be used for calibration only and for no other purpose, unless it can be demonstrated that their performance as reference standards has not been invalidated.

_____ (5) Reference standards of measurement shall be calibrated by a body that can provide traceability to a national standard of measurement. There shall be a program of calibration and verification for reference standards.

_____ (6) Where relevant, reference standards and measuring and testing equipment shall be subjected to in-service checks between calibrations and verifications.

_____ (7) Reference materials shall, where possible, be traceable to national or international standards of measurement, or to national or international standard reference materials.

(h) ***Calibration and test methods***

_____ (1) The laboratory shall have documented instructions on the use and operation of all relevant equipment, on the handling and preparation of items and for calibration and/or testing, where the absence of such instructions could jeopardize the calibrations or tests. All instructions, standards, manuals and reference data relevant to the work of the laboratory shall be maintained up-to-date and be readily available to the staff.

_____ (2) The laboratory shall use appropriate methods and procedures for all calibrations and tests and related activities within its responsibility (including sampling, handling, transport and storage, preparation of items, estimation of uncertainty of measurement and analysis of calibration and/or test data). They shall be consistent with the accuracy required, and with any standard specifications relevant to the calibrations or tests concerned.

NOTES:

(i) Calibration procedures shall contain the required range and tolerance or uncertainty of each item or unit parameter being calibrated or verified. In addition, the procedures shall contain the generic description of the measurement standards and equipment needed with the required parameter, range, tolerances or uncertainties, and specifications for performing the measurement of the calibration or verification, and/or representative types (manufacturer, model, option) that are capable of meeting the generic description for the measurement standards. The procedures shall be consistent with the accuracy required, and with any standard specifications relevant to the calibrations/verifications concerned.

(ii) The laboratory shall ensure that the calibration uncertainties are sufficiently small so that the adequacy of the measurement is not affected. Well-defined and documented measurement assurance techniques or uncertainty analyses may be used to verify the adequacy of a measurement process. If such techniques are not used, then the collective uncertainty of the measurement standards shall not exceed 25% of the acceptable tolerance (e.g., manufacturer's specification) for each characteristic of the measuring and test equipment being calibrated or verified.

_____ (3) Where methods are not specified, the laboratory shall, wherever possible, select methods that have been published in international or national standards, those published by reputable technical organizations or in relevant scientific texts or journals.

_____ (4) Where it is necessary to employ methods that have not been established as standard, these shall be subject to agreement with the client, be fully documented and validated, and be available to the client and other recipients of the relevant reports [see also (k)(2)(x)].

_____ (5) Where sampling is carried out as part of the test method, the laboratory shall use documented procedures and appropriate statistical techniques to select samples [see also (k)(2)(ix)].

_____ (6) Calculations and data transfers shall be subject to appropriate checks.

_____ (7) Where computers or automated equipment are used for the capture, processing, manipulation, recording, reporting, storage or retrieval of calibration or test data, the laboratory shall have written procedures which ensure that:

_____ (i) the NVLAP requirements are complied with;

_____ (ii) computer software, computers or automated equipment is documented and adequate for use;

_____ (iii) procedures are established and implemented for protecting the integrity of data; such procedures shall include, but not be limited to, integrity of data entry or capture, data storage, data transmission and data processing;

_____ (iv) computer and automated equipment is maintained to ensure proper functioning and provided with the environmental and operating conditions necessary to maintain the integrity of calibration and test data [see also (f)(1)];

_____ (v) it establishes and implements appropriate procedures for the maintenance of security of data including the prevention of unauthorized access to, and the unauthorized amendment of, computer records.

_____ (8) Documented procedures shall exist for the purchase, reception and storage of consumable materials used for the technical operations of the laboratory [see also (m)(2)].

(i) ***Handling of calibration and test items***

_____ (1) The laboratory shall have a documented system for uniquely identifying the items to be calibrated or tested, to ensure that there can be no confusion regarding the identity of such items at any time [see also (k)(2)(v)].

_____ (2) Upon receipt, the condition of the calibration or test item, including any abnormalities or departures from standard condition as prescribed in the relevant calibration or test method, shall be recorded. Where there is any doubt as to the item's suitability for calibration or test, where the item does not conform to the description provided, or where the calibration or test required is not fully specified, the laboratory shall consult the client for further instruction before proceeding. The laboratory shall establish whether the item has received all necessary preparation, or whether the client requires preparation to be undertaken or arranged by the laboratory.

_____ (3) The laboratory shall have documented procedures and appropriate facilities to avoid deterioration or damage to the calibration or test item, during storage, handling, preparation, and calibration or test; any relevant instructions provided with the item shall be followed. Where items have to be stored or conditioned under specific environmental conditions, these conditions shall be maintained, monitored and recorded where necessary. Where a calibration or test item or portion of an item is to be held secure (for example, for reasons of record, safety or value, or to enable check calibrations or tests to be performed later), the laboratory shall have storage and security arrangements that protect the condition and integrity of the secured items or portions concerned [see also (e)].

_____ (4) The laboratory shall have documented procedures for the receipt, retention or safe disposal of calibration or test items, including all provisions necessary to protect the integrity of the laboratory.

_____ (5) Tamper-resistant seals shall be affixed to operator-accessible controls or adjustments on measurement standards or measuring and test equipment which, if moved, will invalidate the calibration. The laboratory's calibration system shall provide instructions for the use of such seals and for the disposition of equipment with damaged or broken seals.

NOTE: Tamper-resistant seals are sometimes affixed to equipment to prevent unauthorized access to areas where adjustments or critical components are located.

(j) ***Records***

_____ (1) The laboratory shall maintain a record system to suit its particular circumstances and comply with any applicable regulations. It shall retain on record all original observations, calculations and derived data, calibration records and a copy of the calibration certificate, test certificate or test report for an appropriate period. The records for each calibration and test shall contain sufficient information to permit their repetition. The records shall include the identity of personnel involved in sampling, preparation, calibration or testing [see also (c)(2)(iv)].

EXCEPTION: The retention of all original observations, calculations, and derived data in the calibration record system is not a mandatory requirement for calibration laboratories, although it is encouraged as good laboratory practice.

_____ (2) All records (including those listed in (f)(4) pertaining to calibration and test equipment), certificates and reports shall be safely stored, held secure and in confidence to the client [see also (b)(2)(ix), (c)(2)(xviii)].

NOTE: The period of retention shall be specified in the quality manual.

Record retention time specified: _____

(k) ***Certificates and reports***

_____ (1) The results of each calibration, test, or series of calibrations or tests carried out by the laboratory shall be reported accurately, clearly, unambiguously and objectively, in accordance with any instructions in the calibration or test methods. The results should normally be reported in a calibration certificate, test report or test certificate and should include all the information necessary for the interpretation of the calibration or test results and all information required by the method used [see also (k)(4)].

NOTE: It is recognized that the results of each calibration do not always result in the production of a calibration certificate or report. Whenever a certificate or report is produced, the above requirements shall be met.

(2) Each certificate or report shall include at least the following information:

_____ (i) a title, e.g., "Calibration Certificate," "Test Report" or "Test Certificate";

_____ (ii) name and address of laboratory, and location where the calibration or test was carried out if different from the address of the laboratory;

_____ (iii) unique identification of the certificate or report (such as serial number) and of each page, and the total number of pages;

_____ (iv) name and address of client, where appropriate;

_____ (v) description and unambiguous identification of the item calibrated or tested [see also (i)(1)];

_____ (vi) characterization and condition of the calibration or test item;

_____ (vii) date of receipt of calibration or test item and date(s) of performance of calibration or test, where appropriate;

EXCEPTION: Although it is encouraged as good laboratory practice, the requirement for inclusion of the date received is not mandatory for calibration laboratories.

_____ (viii) identification of the calibration or test method used, or unambiguous description of any non-standard method used;

_____ (ix) reference to sampling procedure, where relevant [see also (h)(5)];

_____ (x) any deviations from, additions to or exclusions from the calibration or test method, and any other information relevant to a specific calibration or test, such as environmental conditions [see also (c)(2)(xv), (h)(4)];

_____ (xi) measurements, examinations and derived results, supported by tables, graphs, sketches and photographs as appropriate, and any failures identified;

_____ (xii) a statement of the estimated uncertainty of the calibration or test result, where relevant;

_____ (xiii) a signature and title, or an equivalent identification of the person(s) accepting responsibility for the content of the certificate or report (however produced), and date of issue [see also (c)(2)(vi)];

_____ (xiv) where relevant, a statement to the effect that the results relate only to the items calibrated or tested;

_____ (xv) a statement that the certificate or report shall not be reproduced except in full, without the written approval of the laboratory;

_____ (xvi) a statement that the report must not be used by the client to claim product endorsement by NVLAP or any agency of the U.S. Government;

_____ (xvii) the signature of an approved signatory for all test and calibration reports endorsed with the NVLAP logo;

▸ _____ (xviii) special limitations of use; and

▸ _____ (xix) traceability statement.

_____ (3) Where the certificate or report contains results of calibrations or tests performed by subcontractors, these results shall be clearly identified [see also (l)].

_____ (4) Particular care and attention shall be paid to the arrangement of the certificate or report, especially with regard to presentation of the calibration or test data and ease of assimilation by the reader. The format shall be carefully and specifically designed for each type of calibration or test carried out, but the headings shall be standardized as far as possible [see also (k)(1)].

_____ (5) Material amendments to a calibration certificate, test report or test certificate after issue shall be made only in the form of a further document, or data transfer including the statement "Supplement to Calibration Certificate (or Test Report or Test Certificate), serial number ... (or as otherwise identified)," or equivalent form of wording. Such amendments shall meet all the relevant requirements of item (j).

_____ (6) The laboratory shall notify clients promptly, in writing, of any event such as the identification of defective measuring or test equipment that casts doubt on the validity of results given in any calibration certificate, test report, or test certificate or amendment to a report or certificate.

NOTE: Such notification shall quantify the magnitude of error created in the calibration results. The laboratory shall notify customers promptly, in writing, of any customer's measuring and test equipment found significantly out of tolerance during the calibration/verification process. Measurement data shall be reported so that appropriate action can be taken.

_____ (7) The laboratory shall ensure that, where clients require transmission of calibration or test results by telephone, telex, facsimile or other electronic or electromagnetic means, staff will follow documented procedures that ensure that the NVLAP requirements are met and that confidentiality is preserved.

_____ (8) Whenever a laboratory accredited by NVLAP issues a calibration or test report which contains data covered by the accreditation and also data not covered by the accreditation, it must clearly identify in its records, and in the report to the client, specifically which calibration or test method(s), or portion of a calibration or test method(s), was not covered by the accreditation. The laboratory must also inform the client, before the fact, when calibrations or tests requested are not covered by the accreditation.

NVLAP policy regarding calibration and test reports issued by an accredited laboratory, which reference the laboratory's accredited status, requires that any

calibration or test report containing data from calibrations or tests which are not covered by the accreditation include:

_____ (i) a statement at the beginning of the report prominently indicating, "This report contains data which are not covered by the NVLAP accreditation"; and

_____ (ii) a clear indication of which data are not covered by the accreditation.

The laboratory must not misrepresent its accreditation. When a client requires or requests accredited services and any of the requested services are not covered by the accreditation, the client must be so advised.

(l) ***Subcontracting of calibration or testing*** [see also (k)(3)]

_____ (1) Where a laboratory subcontracts any part of the calibration or testing, this work shall be placed with a laboratory complying with these requirements. The laboratory shall ensure and be able to demonstrate that its subcontractor is competent to perform the activities in question and complies with the same criteria of competence as the laboratory in respect of the work being subcontracted. The laboratory shall advise the client in writing of its intention to subcontract any portion of the testing to another party.

_____ (2) The laboratory shall record and retain details of its investigation of the competence and compliance of its subcontractors and maintain a register of all subcontracting.

_____ (3) A NVLAP-accredited laboratory intending to subcontract testing or calibration work that will be performed and reported as meeting NVLAP procedures and criteria must:

_____ (i) have in its quality manual a subcontracting policy compatible with the NVLAP policy, with a description of the procedures for administering and implementing those actions to demonstrate the conformance and consistency of the

subcontracted laboratory to perform according to NVLAP procedures;

_____ (ii) place the subcontracted work with a laboratory that maintains accreditation established by NVLAP shown by a current NVLAP Laboratory Code, or provide and maintain current records that demonstrate that the subcontracted laboratory is competent to perform the test(s) or calibration(s) and that it operates in a manner consistent with and in conformance to NVLAP criteria for accreditation;

_____ (iii) clearly identify in its records, and in the report to the client, exactly which data were obtained by the NVLAP-accredited laboratory and which data were obtained by the subcontractor, NVLAP-accredited or not;

_____ (iv) inform its client, before the fact, that it intends to subcontract for completion of all or a portion of the client's work; and

_____ (v) include at the beginning of the report the name, address, and contact person of the subcontracted laboratory(ies), and one of the following statements, as appropriate:

if NVLAP-accredited

"This report contains data which were produced by a subcontracted laboratory **ACCREDITED (NVLAP LAB CODE)** for the calibration or test methods performed"

if not NVLAP-accredited

"This report contains data which were produced by a subcontracted laboratory **NOT ACCREDITED** for the calibration or test methods performed."

The requirements of this section do not supersede any regulation, law, contract specification, or other related conditions which require NVLAP accreditation.

(m) ***Outside support services and supplies***

_____ (1) Where the laboratory procures outside services and supplies in support of calibrations or tests, the laboratory shall use only those outside support services and supplies that are of adequate quality to sustain confidence in the laboratory's calibrations or tests.

_____ (2) Where no independent assurance of the quality of outside support services or supplies is available, the laboratory shall have procedures to ensure that purchased equipment, materials and services comply with specified requirements. The laboratory should, wherever possible, ensure that purchased equipment and consumable materials are not used until they have been inspected, calibrated or otherwise verified as complying with any standard specifications relevant to the calibrations or tests concerned [see also (h)(8)].

_____ (3) The laboratory shall maintain records of all suppliers from whom it obtains support services or supplies required for calibrations or tests.

(n) ***Complaints*** [see also (c)(2)(xvii)]

_____ (1) The laboratory shall have documented policy and procedures for the resolution of complaints received from clients or other parties about the laboratory's activities. A record shall be maintained of all complaints and of the actions taken by the laboratory.

_____ (2) Where a complaint, or any other circumstance, raises doubt concerning the laboratory's compliance with the laboratory's policies or procedures, or with the NVLAP requirements or otherwise concerning the quality of the laboratory's calibrations or tests, the laboratory shall ensure that those areas of activity and responsibility involved are promptly audited in accordance with item (c)(3).

(o) ***Measuring and test equipment (M & TE)***

NOTE: This section applies to the control of measuring and test equipment (M & TE) used to assure that supplies and services comply with prescribed customer requirements. It is based in large part on the requirements found in

government audit standards such as MIL-STD 45662A, and is found in Part II of the ANSI/NCSL Z540-1-1994 (Draft) standard.

(1) General requirements for M & TE

_____ (i) The supplier shall establish and document a system to control the calibration/verification of M & TE.

_____ (ii) M & TE used to determine compliance with customer technical specifications shall be calibrated or verified in accordance with sections 285.33(b) through (n).

_____ (iii) The supplier shall have a program to recall for calibration or verification, or remove from service, M & TE that has exceeded its calibration interval, has broken calibration seals, or is suspected to be malfunctioning because of mishandling, misuse, or unusual results.

_____ (iv) All operations performed by the supplier in compliance with these requirements shall be subject to customer verification at unscheduled intervals.

_____ (v) The supplier shall carry out, or arrange to have carried out, periodic quality auditing of the calibration and verification system in order to ensure its continuing effective implementation and compliance with these requirements.

- Based on the results of the audits and any other relevant factors, such as customer feedback, the supplier shall review and modify the system as necessary.

- Plans and procedures for the audits shall be documented. The conduct of the audit and any subsequent corrective action shall also be documented.

_____ (2) Detailed requirements for M & TE

_____ (i) Calibration system description: The supplier shall provide and maintain a written description of the calibration/verification system covering M & TE and measurement standards. The description shall be sufficient to satisfy each requirement of section 285.33(o) and any deviations shall be submitted with supporting documentation to the customer for approval.

_____ (ii) Adequacy of measurement standards: Measurement standards used by the supplier for calibrating M & TE and other measurement standards shall comply with the requirements of items (f)(1), (g)(1), and (h)(2).

_____ (iii) Environmental conditions: M & TE shall be used in an environment controlled to the extent necessary to ensure valid results. Due consideration shall be given to temperature, humidity, lighting, vibration, dust control, cleanliness, electromagnetic interference and any other factors affecting the results of measurements. Where pertinent, these factors shall be monitored and recorded and, when appropriate, correcting compensations shall be applied to measurement results.

_____ (iv) Intervals of calibration and verification: M & TE requiring calibration shall be calibrated or verified at periodic intervals established and maintained to assure acceptable reliability, where reliability is defined as the probability that M & TE will remain in-tolerance throughout the interval. Intervals shall be established for all M & TE requiring calibration unless the equipment is regularly monitored through the use of check standards in a documented measurement assurance process. Check standards must closely represent the item parameters normally tested in the process and the check standard must be verified periodically. Where intervals are used to ensure reliability, the interval setting system must be systematically applied and shall have stated reliability goals and a method of verifying that the goals are being attained. Intervals may be based on usage or time since last calibration or verification. All exemptions from periodic calibration or verification shall be documented. The recall system may provide for the temporary extension of the calibration due date for limited periods of time under specified conditions that do not unreasonably impair the satisfaction of the customer's requirements.

_____ (v) Calibration procedures: Procedures used to calibrate/verify the supplier's M & TE shall comply with the requirements of items (h)(1) and (h)(2).

_____ (vi) Out-of-tolerance conditions: If any M & TE is found to be significantly out of tolerance during the calibration/verification process, the supplier's system shall provide for notification to the user and to the supplier's quality element, if appropriate, of the out-of-tolerance condition with the associated measurement data so that appropriate action can be taken.

_____ (vii) Adequacy of calibration system: The supplier shall establish and maintain documented procedures to evaluate the adequacy of the calibration system and to ensure compliance with these requirements.

_____ (viii) Calibration sources: M & TE requiring calibration shall be calibrated or verified by laboratories that comply with sections 285.33(b) through (n).

_____ (ix) Records: These requirements shall be supported by records documenting

that established schedules and procedures are followed to maintain the adequacy of all M & TE. The records for M & TE requiring calibration shall include an individual record of calibration or verification, or other means of control, providing a description or identification of the item, calibration interval, date calibrated, identification of the calibration source, calibration results (data and/or condition status) and calibration action taken (adjusted, repaired, new value assigned, derated, etc.).

_____ (x) Calibration status: M & TE shall be labeled to indicate calibration or verification status. The label shall identify specific date calibrated (day, month, year, Julian date, or equivalent) and the specific calibration due date or usage equivalent. Items not calibrated to their full capability or which have other limitations of use, shall be labeled or otherwise identified as to the limitations. When it is impractical to apply a label directly to an item, the label may be affixed to the instrument container or some other suitable means may be used to reflect calibration status. Tamper-resistant seals are affixed to operator accessible controls or adjustments which if moved will invalidate the calibration. The quality system shall provide instructions for the disposition of equipment with broken tamper-resistant seals.

_____ (xi) Control of subcontractor calibration: The supplier is responsible for assuring that the subcontractor's calibration system conforms to section 285.33 (l) to the degree necessary to assure compliance with contractual requirements. NVLAP accreditation of the subcontractor's laboratory can serve as the basis for compliance with this requirement.

_____ (xii) Storage and handling: M & TE shall be handled, stored, and transported in a manner which shall not adversely affect the calibration or condition of the equipment.

NVLAP LAB CODE:

GENERAL OPERATIONS CHECKLIST - COMMENTS AND DEFICIENCIES

Instructions to the Assessor: Use this sheet to document comments and deficiencies. For each, identify the appropriate item number from the checklist. Identify comments with a "C" and deficiencies with an "X." If additional space is needed, make copies of this page (or use additional blank sheets).

Item No.	***Comments and/or Deficiencies***

NVLAP LAB CODE:

GENERAL OPERATIONS CHECKLIST - COMMENTS AND DEFICIENCIES

Instructions to the Assessor: Use this sheet to document comments and deficiencies. For each, identify the appropriate item number from the checklist. Identify comments with a "C" and deficiencies with an "X." If additional space is needed, make copies of this page (or use additional blank sheets).

Item No.	***Comments and/or Deficiencies***

APPENDIX C

SPECIFIC OPERATIONS CHECKLIST

National Voluntary Laboratory Accreditation Program (NVLAP)
for
Information Technology Security Testing - Common Criteria Testing

SPECIFIC OPERATIONS ON-SITE CHECKLIST

Abstract

This checklist is designed for use by NVLAP Technical Expert(s) during the conduct of an on-site assessment for initial or renewal of accreditation for Common Criteria Testing (CCT). The checklist contains items from the Program Handbook, NVLAP Procedures, and technical references. The checklist is organized into sections similar to the Program Handbook and Procedures.

The completed checklist becomes a part of the laboratory ON-SITE ASSESSMENT REPORT that is used in the evaluation of the laboratory for granting or renewal of accreditation. Deficiencies noted in this checklist must be resolved in accordance with the NVLAP Procedures. Comments not specified as deficiencies may be directed to the laboratory.

Laboratory Name _____

NVLAP Technical Expert(s) _____

On-Site Dates _____

Instructions to Laboratory

Respond in writing within 30 days of the date of this report, addressing all deficiencies documented by the assessor. Each deficiency must be referenced, in your response, by number as it is listed in the report.

This on-site assessment report conveys the opinion of the assessor as a single representative of NVLAP. The final evaluation of your laboratory for the purpose of recommending approval or denial of accreditation will be conducted by NIST evaluators who will review this report, the written information submitted by you, and results of any required proficiency testing. You must respond to this report by identifying the actions you have taken, or plan to take, to correct the deficiencies identified. Respond in detail so that an accurate evaluation can be completed. Failure to respond may delay an accreditation decision. Questions concerning this report should be directed to NVLAP.

The assessor has discussed the contents of this report with members of the laboratory management who agree to respond in writing to NIST, regarding resolution or correction of any deficiencies noted, within 30 days of the date of this report.

_____	_____	
Signature of Authorized Representative or designee	Printed Name	Date

CCT-SPECIFIC OPERATIONS CHECKLIST

Instructions to the Assessor: This checklist addresses specific criteria prescribed in Section 285.33 of the Information Technology Security Testing - Common Criteria Handbook. These criteria supplement and **do not** supersede the *Criteria for Accreditation*, based on Section 285.33 of the NVLAP Procedures, which are addressed in the NVLAP GENERAL OPERATIONS CHECKLIST.

Place an "X" beside any of the following items that represent a NVLAP deficiency. Place a "C" beside each item on which you are commenting for other reasons. Record the item number and your deficiency explanation and/or comments directly in this checklist or on the Comments and Deficiencies sheets at the end of this checklist. If the Comments and Deficiencies sheets are used, be sure to unambiguously identify the question or item to which you are referring.

Place a check beside all other items you observed or verified at the laboratory. All items observed or verified must be marked.

SEC. 285.33 CRITERIA FOR ACCREDITATION

Item No. Comments and/or Deficiencies

(b) Organization and Management:

(1) The Laboratory shall:

_____ (i) establish and maintain policies and procedures for maintaining laboratory impartiality and integrity in the conduct of IT security evaluations, such that

- the same laboratory member or team cannot develop and evaluate the same Protection Profile, Security Target, or IT product, and
- the same laboratory member cannot provide consulting services for and then participate in the evaluation of the same Protection Profile, Security Target, or IT product;

_____ (ii) ensure that its personnel are free from any commercial, financial, or other pressures that might adversely affect the impartiality of their work;

_____ (iii) be organized in such a way that confidence in its independence of judgment and integrity is maintained at all times;

_____ (iv) have an explicit policy and set of procedures for maintaining separation, both physical and electronic, between the laboratory evaluators and product developers, system integrators, and others who may have an interest in and may unduly influence the evaluation outcome;

_____ (v) have procedures that support effective communication within the laboratory, between the laboratory and its customers (e.g., vendors, sponsors, and the NIAP Validation Body), and with the general public.

(c) Quality system, audit and review:

(1) Quality system requirements:

_____ (i) The laboratory must maintain a quality system that fully documents the laboratory's policies, practices, and the specific steps taken to ensure the quality of the IT security evaluations.

_____ (ii) The quality system must provide for periodic reviews of the competence of the staff involved in the conduct of security evaluations.

_____ (iii) Reference documents, standards, and publications available as references in developing and maintaining the quality system and for use by laboratory staff include:

_____ (a) NIST Handbook 150, *NVLAP Procedures and General requirements*;

_____ (b) NIST Special Publication 810, *NVLAP Directory*;

_____ (c) NIST Handbook 150-20, *Information Technology Security Testing - Common Criteria*;

_____ (d) *NIAP Common Criteria Evaluation and Validation Scheme for Information Technology Security: Organization, Management, and Concept of Operations (Scheme Publication #1);*

_____ (e) *Common Criteria for Information Technology Security Evaluation;*

_____ (f) *Common Methodology for Information Technology Security Evaluation*

_____ (iv) Records must be kept of all quality system activities.

_____ (v) The laboratory shall establish and maintain documented procedures for the review of contracts between itself and its clients. The contract review shall be conducted to ensure that the laboratory is capable of providing the service and that the requirements, rights, and responsibilities of the parties are understood.

(2) Quality manual requirements:

(i) The laboratory must have a quality manual that contains or refers to, at a minimum (in addition to the quality manual requirements levied by NIST Handbook 150):

_____ (a) a description and details of the laboratory's implementation of the CCT accreditation requirements;

_____ (b) policies and procedures to ensure the protection of proprietary information, to address at a minimum how proprietary information will be protected from non-laboratory personnel, laboratory visitors, laboratory personnel without a need to know, and from other unauthorized persons;

_____ (c) the laboratory's procedures for software handling and integrity; and

_____ (d) additional procedures for conducting evaluations at client sites, if applicable.

_____ (3) The laboratory shall conduct audits and management reviews on a periodic basis.

(d) Personnel:

(1) The Laboratory shall:

_____ (i) maintain a competent administrative and technical staff appropriate for Common Criteria-based IT security evaluations;

_____ (ii) maintain position descriptions and resumes for the laboratory staff members who conduct security evaluations and responsible supervisory personnel;

_____ (iii) maintain a list of personnel designated to fulfill NVLAP requirements, including laboratory director, authorized representative, approved signatories, and key technical personnel;

_____ (iv) identify a staff member as quality manager who has overall responsibility for the quality system and maintenance of the quality manual; and

_____ (v) document the required qualifications for each staff position involved in the IT security evaluation process;

_____ (vi) have a detailed documented description of its training program for new and current staff members. Each new staff member must be trained for assigned duties. The training program must be updated and current staff members must be retrained when the *Common Criteria*, *Common Methodology*, or scope of accreditation changes, or when the individuals are assigned new responsibilities;

_____ (vii) keep training materials that are maintained within the laboratory up-to-date;

_____ (viii) review the competence of each staff member for each test method the staff member is authorized to conduct. The immediate supervisor, or a designee appointed by the laboratory director, must conduct annually an assessment and an observation of performance for each staff member. A record of the annual review of each staff member must be dated and signed by the supervisor and the employee; and

_____ (ix) maintain a description of competency review programs in the quality manual.

_____ (2) Laboratory staff members who conduct IT security evaluation activities shall have a Bachelor of Science in Computer Science, Computer Engineering, or related technical discipline or equivalent experience.

_____ (3) Laboratory staff collectively shall have knowledge or experience in the following areas: demonstrated coursework and/or experience in operating systems, data structures, design/analysis of algorithms, database systems, programming languages, computer systems architectures, and networking.

(4) Staff members shall be trained in the following areas:

_____ (i) general requirements of the test methods including generation of evaluation reports;

_____ (ii) computer science concepts;

_____ (iii) computer security concepts;

_____ (iv) working knowledge of the *Common Criteria;* and

_____ (v) working knowledge of the *Common Methodology*.

(e) Accommodation and environment:

(1) The Laboratory shall:

_____ (i) have adequate facilities to conduct IT security evaluations. This includes facilities for security evaluation, staff training, record keeping, document storage, and software storage;

_____ (ii) have a proprietary protection system to safeguard client proprietary hardware, software, test data, electronic and paper records, and other materials. This system must protect the proprietary materials from personnel outside the laboratory, visitors to the laboratory, laboratory personnel without a need to know, and other unauthorized persons;

_____ (iii) isolate laboratory networks used to conduct IT security evaluations from those outside the laboratory;

_____ (iv) have electronic mail capability for communications with the NIAP Validation Body;

_____ (v) have Internet access for obtaining revisions to the *Common Criteria*, *Common Methodology*, guidance, and interpretations;

_____ (vi) have an effective virus protection and software/data backup program;

_____ (vii) have a system for conducting security evaluations at client sites or other non-laboratory facilities such that the same constraints applicable to the laboratory environment are maintained. The laboratory shall control the evaluation environment in such a way that unauthorized entities do not gain access to the system on which the evaluation is conducted during evaluation; and

_____ (viii) maintain a system of separation between products of different clients and evaluations, to include the product under evaluation, the test platform, peripherals, and documentation.

(f) Equipment and reference material:

(1) The Laboratory shall:

_____ (i) maintain on-site systems adequate to support IT security evaluations;

_____ (ii) have an electronic report generation capability;

_____ (iii) document and maintain records on all test equipment or test suites within its control, to include customer-supplied and laboratory-supplied equipment; and

_____ (iv) be knowledgeable in the configuration and operation of all equipment under its control.

(g) Measurement traceability and calibration:

(1) The Laboratory shall:

_____ (i) maintain the equipment used for conducting security evaluations:

- In accordance with the manufacturer's recommendations; or
- In accordance with internally-documented laboratory procedures, as applicable.

_____ (ii) calibrate their test equipment;

_____ (iii) document the reference standards used and the environmental conditions at the time of calibration; and

_____ (iv) verify that tests conducted using test tools or equipment and the results they generate are traceable to the evaluator actions in the *Common Criteria* and *Common Methodology*.

(h) Calibration and test methods:

(1) The Laboratory shall:

_____ (i) comply with NIAP-specified guidance and interpretations of the evaluation criteria within the specified timeframe if evaluation validation is desired;

_____ (ii) have documented procedures for conducting security evaluations using the *Common Criteria* and *Common Methodology* and ensure that these procedures are being followed;

_____ (iii) maintain the Common Criteria, Common Methodology, NIAP guidance and interpretations, and the laboratory's procedures for conducting security evaluations up-to-date and have them readily available to the staff;

_____ (iv) ensure that only laboratory personnel perform all actions necessary to conduct the tests and record the results when evaluations are conducted at non-laboratory sites; and

_____ (v) have additional procedures regarding the conduct of evaluations at non-laboratory facilities to ensure that the same requirements beholden to the laboratory and its facility are maintained, as applicable.

(j) Records:

(1) The Laboratory shall:

_____ (i) maintain a functional record-keeping system for each security evaluation.

_____ (a) Records must be easily accessible and contain complete information on the evaluation.

_____ (b) Records of evaluation activities must be traceable to *Common Criteria* evaluator actions and *Common Methodology* work units.

_____ (c) Computer-based media must be logged and properly marked, and there must be proper back up.

_____ (d) Entries in laboratory notebooks must be dated and signed or initialed.

_____ (e) Computer-based records must contain entries of pertinent staff/date information as required in the quality manual, as well as be maintained in accordance with laboratory guidelines and in a manner that ensures record integrity preservation;

_____ (ii) maintain, release, and destroy laboratory records in accordance with the laboratory's proprietary information policy and contractual agreements with clients;

_____ (iii) retain records for a period of at least five years;

_____ (iv) maintain a policy and set of procedures for ensuring record accuracy and integrity; and

_____ (v) take steps to ensure no unauthorized entity can gain access to the physical or on-line records either during or after the evaluation.

(2) Records covering the following are required and will be reviewed during the on-site assessment by selective sampling:

_____ (i) quality system;

_____ (ii) staff training dates and competency reviews;

_____ (iii) NVLAP proficiency test dates and results;

_____ (iv) software versions and updates;

_____ (v) statement of policy and conditions for evaluation;

_____ (vi) evaluation methods and procedures;

_____ (vii) acceptance/rejection of products submitted for evaluation;

_____ (viii) comprehensive logs for tracking samples and evaluation activities;

_____ (ix) evaluation data (including any diagrams, photos, and graphic images) and official reports;

_____ (x) calibration of test tools and equipment;

_____ (xi) audits and management reviews;

_____ (xii) test files; and

_____ (xiii) equipment.

(3) Evaluation equipment, test tools and equipment, and calibration records should include the following:

_____ (i) equipment name or description;

_____ (ii) model, style, or serial number;

_____ (iii) manufacturer;

_____ (iv) notation of all equipment variables requiring calibration;

_____ (v) the range of calibration;

_____ (vi) the resolution of the instrument and its allowable error, as applicable;

_____ (vii) calibration date and schedule;

_____ (viii) date and result of last calibration;

_____ (ix) identity of the laboratory individual or external service responsible for calibration; and

_____ (x) source of reference standard and traceability.

(k) Certificates and reports:

(1) The Laboratory shall:

_____ (i) issue evaluation reports of its work that accurately, clearly, and unambiguously present the evaluation conditions, evaluation setup, evaluation results, and all

required information;

_____ (ii) provide evidence to support the results of the IT security evaluations;

_____ (iii) identify and mark comments and results that are outside the scope of the test methods for which the laboratory is accredited.

(2) Evaluation reports:

_____ (i) must contain sufficient information for the exact test conditions to be reproduced at a later time if a retest is necessary;

_____ (ii) if produced for submission to NIAP, must meet the requirements of the Common Criteria Scheme;

_____ (iii) if delivered to NIAP via electronic transfer technology, must be digitally signed or have a message authentication code applied to ensure integrity of the report and the identity of the laboratory. and the laboratory shall:

_____ (a) provide a secure means of conveying the necessary information to NIAP for digital signature or message authentication code verification;

_____ (b) employ a confidentiality mechanism to ensure that the evaluation report cannot be disclosed to anyone other that the intended recipient; and

_____ (c) provide a secure means of conveying the necessary information to NIAP; and

_____ (v) if produced for submission to NIAP, must be changed in accordance with NIAP requirements.

_____ (vi) if produced for purposes other that validation, shall have corrections or additions only by a further document suitable marked.

_____ (a) If the change involves a *Common Criteria* requirement, this document must specify which *Common Criteria* requirement is in question, the content of the result, the explanation of the result, and the reason for acceptance of the result.

LABORATORY PERSONNEL CHECKLIST 961004

Notes to the Assessor: Please use a separate copy of this checklist to document the evaluation of the competence and experience of laboratory personnel. It is not necessary to explicitly ask each of the questions.

NIST Handbook 150, Sec. 285.33 Criteria for accreditation, (b) Organization and management, (2) The laboratory shall: (i) have managerial staff with the authority and resources needed to discharge their duties; (vi) have a technical manager (however named) who has overall responsibility for the technical operations;.

NIST Handbook 150, Sec. 285.33 Criteria for accreditation, (b) Organization and management, (2) The laboratory shall: (vii) have a quality manager (however named) who has responsibility for the quality system and its implementation ....

NIST Handbook 150, Sec. 285.5 Definitions, Approved Signatory (of an accredited laboratory): An individual who is recognized by NVLAP as competent to sign accredited laboratory calibration or test reports. NOTE: The Approved Signatory is responsible for technical content of the report ....

Interview with: Technical Manager__, Quality Manager__, Approved Signatory(s)_

_____ 1.1 Staff member's name:

_____ 1.2 Job title:

_____ 1.3 Ask the staff member to describe his/her duties as they relate to the laboratory.

_____ 1.4 Is the description given by the staff member consistent with what is in the personnel records, résumé, and quality system documentation?

_____ 1.5 Discuss the following staff functions and their relationship to this staff member:

NVLAP Authorized Representative
Technical Manager
Deputy Technical Manager
Quality Manager
Approved Signatory
Test Operations
Systems Management
Recordkeeping/Librarian

_____ 1.6 Does the staff member have other duties or responsibilities which are not a part of the laboratory? Do these additional responsibilities conflict with test laboratory responsibilities? If so, how?

_____ 1.7 Is the staff member familiar with the relevant technical, testing, product and quality standards? Ask the staff member to give an overview of the process that they are responsible for.

_____ 1.8 Discuss the following:

What do you understand by "quality in testing"?

How do you ensure repeatability and reproducibility?
(a) consistently by different members of staff?
(b) consistently over different test methods?
(c) consistently over time by the same staff?

Quality Manager - Internal Audits:

_____ 1.9 Are there procedures for performing formal quality audits of the laboratory? Are there procedures for performing informal quality audits of the laboratory?

_____ 1.10 When was the last formal internal quality audit performed? How often are they performed? When was the last informal quality audit performed? How often are they performed?

_____ 1.11 Were there any deficiencies found? Have the deficiencies been resolved? Has this been documented? What is the policy for time spans for resolution of deficiencies?

Approved Signatories:

_____ 1.12 Is the Approved Signatory appropriate for the task and competent to accomplish it? Does the laboratory have appropriate procedures for designating Approved Signatories? Is the Scope of Accreditation for which the Approved Signatory is designated properly documented?

APPENDIX D

TEST METHOD SELECTION LIST

INFORMATION TECHNOLOGY SECURITY TESTING
TEST METHOD SELECTION LIST – COMMON CRITERIA TESTING

Instructions: Check 26/A01 and each test method for which you are requesting accreditation. Minimum test methods required for 26/A01 accreditation are APE, ASE, and EAL1.

COMMON CRITERIA TESTING (CCT)

	NVLAP Test Method Code	***Test Method Designation***
_____	26/A01	ISO/IEC FDIS 15408: Common Criteria for Information Technology Security Evaluation CEM-97/017: Common Evaluation Metholology for Information Technology Security, Part 1 – Introduction and general model CEM-99/008: Common Methodology for Information Technology Security Evaluation, Part 2 – Evaluation methodology
_____	26/A01a	**APE:** Protection Profile evaluation
_____	26/A01b	**ASE:** Security Target evaluation
_____	26/A01c	**EAL1:** Evaluation assurance level 1
_____	26/A01d	**EAL2:** Evaluation assurance level 2
_____	26/A01e	**EAL3:** Evaluation assurance level 3
_____	26/A01f	**EAL4:** Evaluation assurance level 4